This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **07038599 A**

(43) Date of publication of application: **07 . 02 . 95**

(51) Int. Cl **H04L 12/46**
H04L 12/28
G06F 13/00
G06F 15/16

(21) Application number: **05179404**

(22) Date of filing: **20 . 07 . 93**

(71) Applicant: **TOSHIBA CORP**

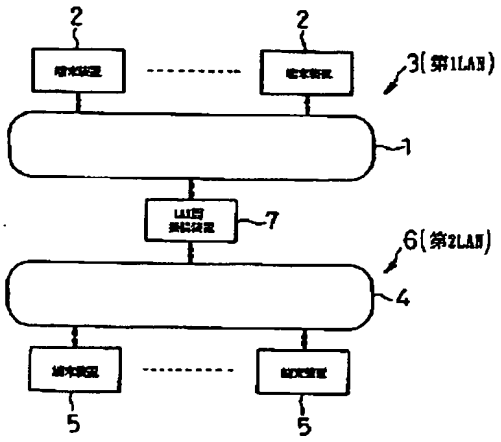
(72) Inventor: **TATARA HIROYUKI**

(54) **INTER-LAN CONNECTOR**

(57) Abstract:

PURPOSE: To prevent data from being illegally accessed from a LAN on a low security side to a LAN on a high security side when connecting the LAN at different security levels.

CONSTITUTION: When the data are accessed from each terminal equipment 5 constituting a second LAN 6 at the high security level to each terminal equipment 2 constituting a first LAN 3 at the low security level, this is detected by the transport layer of an inter-LAN connector 7, the data access between these respective terminal equipments 2 and 5 is supported, when the data are oppositely accessed from each terminal equipment 2 to each terminal equipment 5, this is detected by the transport layer of the inter-LAN connector 7, and the data access between these respective terminal equipments 2 and 5 is inhibited.



COPYRIGHT: (C)1995,JPO

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平7－38599

(43)公開日　平成７年(1995)２月７日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ	12/46				
	12/28				
Ｇ０６Ｆ	13/00	３５１　Ｚ	7368－5B		
	15/16	４７０　Ｍ	7429－5L		
			8732－5K	Ｈ０４Ｌ　11/ 00　３１０　Ｃ	

審査請求　未請求　請求項の数１　ＯＬ　（全 ９ 頁）

(21)出願番号　特願平5－179404

(22)出願日　平成５年(1993)７月20日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　多々良　裕之
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内

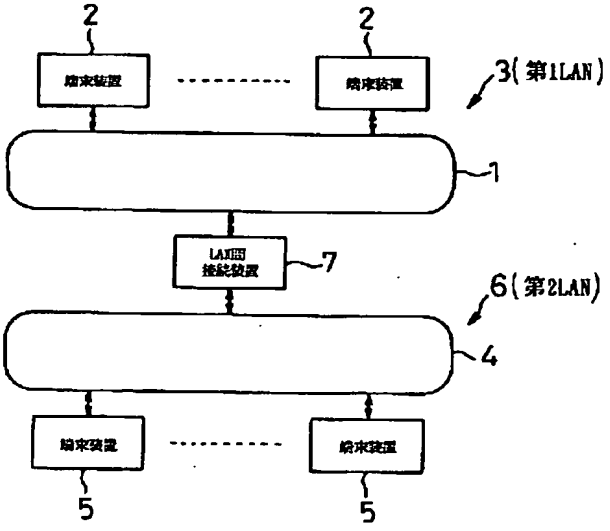
(74)代理人　弁理士　三好　秀和　（外３名）

(54)【発明の名称】　ＬＡＮ間接続装置

(57)【要約】

【目的】　本発明はセキュリティレベルが異なるＬＡＮ間を接続するとき、低セキュリティレベル側のＬＡＮから高セキュリティレベル側のＬＡＮに対する不正なデータアクセスを防止する。

【構成】　セキュリティレベルが高い第２ＬＡＮ６を構成する各端末装置５からセキュリティレベルが低い第１ＬＡＮ３を構成する各端末装置２に対するデータアクセスがあったとき、ＬＡＮ間接続装置７のトランスポート層２３によってこれを検出してこれらの各端末装置２、５間のデータアクセスをサポートし、逆に前記各端末装置２から前記各端末装置５に対するデータアクセスがあったとき、ＬＡＮ間接続装置７のトランスポート層２３によってこれを検出してこれらの各端末装置２、５間のデータアクセスを禁止する。



1

【特許請求の範囲】

【請求項１】　ＯＳＩ規格によって指定された複数の層を有し、セキュリティが高く設定された高セキュリティＬＡＮと、ＯＳＩ規格によって指定された複数の層を有し、セキュリティが低く設定された低セキュリティＬＡＮとを接続するＬＡＮ間接続装置において、

処理層としてＯＳＩ規格の物理層、データリンク層、ネットワーク層、トランスポート層を備え、

低セキュリティＬＡＮを構成する端末装置の１つから高セキュリティＬＡＮを構成する端末装置に対して接続要求が出されたとき、前記トランスポート層によってこれを取り込んで接続要求のＴＣＰフォーマットおよびこのＴＣＰフォーマット中の確立要求フラグの有無を確認し、接続要求を出した端末装置と、接続先として指定された端末装置との間のコネクションを禁止し、

高セキュリティＬＡＮを構成する端末装置の１つから低セキュリティＬＡＮを構成する端末装置に対して接続要求が出されたとき、前記トランスポート層によってこれを取り込んで接続要求のＴＣＰフォーマットおよびこのＴＣＰフォーマット中の確立要求フラグの有無を確認し、正しい接続要求であれば、接続要求を出した端末装置と、接続先として指定された端末装置との間のコネクションを確立してデータ通信を行なわせる、

ことを特徴とするＬＡＮ間接続装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は複数のＬＡＮを接続して情報処理ネットワークシステムを構築するとき使用されるＬＡＮ間接続装置に関する。

【０００２】

【従来の技術】ＬＡＮ間接続装置を使用して複数のＬＡＮを相互に接続した情報処理ネットワークシステムとして、従来、図５に示すシステムが知られている。

【０００３】この図に示す情報処理ネットワークシステムは１つのケーブル１０１およびこのケーブル１０１に接続される複数の端末装置１０２によって構成される第１ＬＡＮ１０３と、１つのケーブル１０４およびこのケーブル１０４に接続される複数の端末装置１０５によって構成される第２ＬＡＮ１０６と、これら第１、第２ＬＡＮ１０３、１０６を相互に接続するＬＡＮ間接続装置１０７とを備えており、第１、第２ＬＡＮ１０３、１０６に接続されている各端末装置１０２、１０５間でデータの授受を行なって各種のデータ処理を行なう。

【０００４】前記第１、第２ＬＡＮ１０３、１０６は各々、図６に示す如くＯＳＩ規格によって物理層１１０、データリンク層１１１、ネットワーク層１１２、トランスポート層１１３、セション層１１４、プレゼンテーション層１１５、応用層１１６の７層によって構成されており、このＯＳＩ規格によって異機種のコンピュータ動作を自由に、かつ相互に接続し得るようにされている。

2

【０００５】また、ＬＡＮ間接続装置１０７は物理層１２０、データリンク層１２１、ネットワーク層１２２の３層によって構成されており、これらの物理層１２０～ネットワーク層１２２によって第１ＬＡＮ１０３の各端末装置１０２と、第２ＬＡＮ１０６の各端末装置１０５とのデータ通信を相互にサポートする。

【０００６】そして、第１ＬＡＮ１０３を構成する端末装置１０２の１つから第２ＬＡＮ１０６を構成する端末装置１０５に対して接続要求を出したとき、図７に示す如くＬＡＮ間接続装置１０７によってこれを取り込んで接続要求を出した端末装置１０２と、接続先として指定された端末装置１０５との間のコネクションを確立してデータ通信を行なわせる。

【０００７】同様に、第２ＬＡＮ１０６を構成する端末装置１０５の１つから第１ＬＡＮ１０３を構成する端末装置１０２に対して接続要求を出したとき、ＬＡＮ間接続装置１０７によってこれを取り込んで接続要求を出した端末装置１０５と、接続先として指定された端末装置１０２との間のコネクションを確立してデータ通信を行なわせる。

【０００８】これによって、第１、第２ＬＡＮ１０３、１０６の各端末装置１０２、１０５によって第１、第２ＬＡＮ１０３、１０６を構成する他の各端末装置１０２、１０５内のデータを参照したり、より大規模なデータ処理を可能にしたりしている。

【０００９】

【発明が解決しようとする課題】しかしながら、上述した従来のＬＡＮ間接続装置１０７を使用した情報処理ネットワークシステムにおいては、次に述べるような問題があった。

【００１０】すなわち、第１ＬＡＮ１０３または第２ＬＡＮ１０６の各セキュリティレベルを異なった値にしている場合、例えば第１ＬＡＮ１０３のセキュリティレベルを低くし、第２ＬＡＮ１０６のセキュリティレベルを高くしているとき、第２ＬＡＮ１０６自体のセキュリティレベルを高くし、この第２ＬＡＮ１０６を構成する各端末装置１０５間のデータ通信を制限していても、第１ＬＡＮ１０３を構成する各端末装置１０２によって第２ＬＡＮ１０６を構成する各端末装置１０５内のデータが取り込まれて第２ＬＡＮ１０６のセキュリティが破られてしまうという保管管理上の問題があった。

【００１１】そこで、このような問題を解決する方法として、ＬＡＮ間接続装置１０７によって送信元アドレスと、宛先アドレスとを確認して第１ＬＡＮ１０３と第２ＬＡＮ１０６との間のデータ中継を制限する方法も試みられているが、このような方法では、アドレスが不正に改ざんされたとき、セキュリティが破られてしまうという問題があり、決定的な解決には至っていないのが現状である。

【００１２】本発明は上記の事情に鑑み、セキュリティ

レベルが異なるＬＡＮ間を接続するとき、セキュリティレベルが低い方のＬＡＮからセキュリティレベルが高い方のＬＡＮに対する不正なデータアクセスを防止し、これによってセキュリティレベルが高く設定されているＬＡＮのデータが外部に漏れないようにすることができるＬＡＮ間接続装置を提供することを目的としている。

【００１３】

【課題を解決するための手段】上記の目的を達成するために本発明は、ＯＳＩ規格によって指定された複数の層を有し、セキュリティが高く設定された高セキュリティＬＡＮと、ＯＳＩ規格によって指定された複数の層を有し、セキュリティが低く設定された低セキュリティＬＡＮとを接続するＬＡＮ間接続装置において、処理層としてＯＳＩ規格の物理層、データリンク層、ネットワーク層、トランスポート層を備え、低セキュリティＬＡＮを構成する端末装置の１つから高セキュリティＬＡＮを構成する端末装置に対して接続要求が出されたとき、前記トランスポート層によってこれを取り込んで接続要求のＴＣＰフォーマットおよびこのＴＣＰフォーマット中の確立要求フラグの有無を確認し、接続要求を出した端末装置と、接続先として指定された端末装置との間のコネクションを禁止し、高セキュリティＬＡＮを構成する端末装置の１つから低セキュリティＬＡＮを構成する端末装置に対して接続要求が出されたとき、前記トランスポート層によってこれを取り込んで接続要求のＴＣＰフォーマットおよびこのＴＣＰフォーマット中の確立要求フラグの有無を確認し、正しい接続要求であれば、接続要求を出した端末装置と、接続先として指定された端末装置との間のコネクションを確立してデータ通信を行なわせることを特徴としている。

【００１４】

【作用】上記の構成において、処理層としてＯＳＩ規格の物理層、データリンク層、ネットワーク層、トランスポート層を備え、低セキュリティＬＡＮを構成する端末装置の１つから高セキュリティＬＡＮを構成する端末装置に対して接続要求が出されたとき、前記トランスポート層によってこれを取り込んで接続要求のＴＣＰフォーマットおよびこのＴＣＰフォーマット中の確立要求フラグの有無を確認し、接続要求を出した端末装置と、接続先として指定された端末装置との間のコネクションを禁止し、高セキュリティＬＡＮを構成する端末装置の１つから低セキュリティＬＡＮを構成する端末装置に対して接続要求が出されたとき、前記トランスポート層によってこれを取り込んで接続要求のＴＣＰフォーマットおよびこのＴＣＰフォーマット中の確立要求フラグの有無を確認し、正しい接続要求であれば、接続要求を出した端末装置と、接続先として指定された端末装置との間のコネクションを確立してデータ通信を行なわせることにより、セキュリティレベルが異なるＬＡＮ間を接続するとき、セキュリティレベルが低い方のＬＡＮからセキュリティレベルが高い方のＬＡＮに対する不正なデータアクセスを防止し、これによってセキュリティレベルが高く設定されているＬＡＮのデータが外部に漏れないようにする。

【００１５】

【実施例】図１は本発明によるＬＡＮ間接続装置の一実施例を使用した情報処理ネットワークシステムの一例を示すブロック図である。

【００１６】この図に示す情報処理ネットワークシステムは１つのケーブル１およびこのケーブル１に接続される複数の端末装置２によって構成され、セキュリティレベルが低く設定される第１ＬＡＮ３と、１つのケーブル４およびこのケーブル４に接続される複数の端末装置５によって構成され、セキュリティレベルが高く設定される第２ＬＡＮ６と、これら第１、第２ＬＡＮ３、６を相互に接続するＬＡＮ間接続装置７とを備えており、第１ＬＡＮ３を構成する端末装置２間でデータの授受を行なって各種のデータ処理を行なうとともに、第２ＬＡＮ６を構成する端末装置５間でデータの授受を行なって各種のデータ処理を行ない、さらに第２ＬＡＮ６を構成する各端末装置５から第１ＬＡＮ３を構成する各端末装置２に対するデータアクセスをサポートし、逆に第１ＬＡＮ３を構成する各端末装置２から第２ＬＡＮ６を構成する各端末装置５に対するデータアクセスを禁止する。

【００１７】前記第１、第２ＬＡＮ３、６は各々、図２に示す如くＯＳＩ規格によって物理層１０、データリンク層１１、ネットワーク層１２、トランスポート層１３、セション層１４、プレゼンテーション層１５、応用層１６の７層によって構成されており、このＯＳＩ規格によって異機種のコンピュータ動作を自由に、かつ相互に接続し得るようにされている。

【００１８】また、ＬＡＮ間接続装置７は物理層２０、データリンク層２１、ネットワーク層（ＩＰ層）２２、トランスポート層（ＴＣＰ層）２３の４層によって構成されており、これらの物理層２０～トランスポート層２３によって第２ＬＡＮ６の各端末装置５から第１ＬＡＮ３の各端末装置２に対するデータアクセスをサポートしている。

【００１９】この場合、図３に示す如くこれら第１、第２ＬＡＮ３、６およびＬＡＮ間接続装置７を構成する各物理層１０、２０はＯＳＩ参照モデルの第１層を構成する層であり、同軸ケーブルや光ファイバ、通信衛星の採用、アナログ伝送方式に加え、デジタル伝送の導入などにより、データの伝送路、すなわち通信媒体の多様化が進んでいることから、この多様な通信媒体の制御機能を物理層として分離して、通信媒体の選択の自由度を増すために設けられている。

【００２０】また、データリンク層１１、２１はＯＳＩ参照モデルの第２層にあたる層であり、１本の通信媒体上で単位データを転送する際、通信媒体の誤り品質や形

状（直通、分岐、ループなど）などに対して特別の制御技術が必要になることから、今後、光ファイバや通信衛星の普及に対応して、従来のデータリンク制御手順（ＨＤＬＣやベーシック手順など）に代わり、特有の最適なデータリンク制御手順が開発される可能性があり、通信媒体の制御（物理層）とその上のデータリンク転送制御を別々の機能層としておくことが適切であることから設けられている。

【００２１】また、ネットワーク層１２、２２はＯＳＩ参照モデルの第３層にあたる層であり、一般に大規模で複雑な構成のコンピュータネットワークにおいては、通信の終端として動作する開放型システム（すなわち、応用プロセスが存在する開放型システム）間には、並列あるいは直列に使用されている通信回線網や、通信の中継の役割を果たす開放型システムが存在し、またある開放型システムが終端開放型システムとしても、中間開放型システムとしても動作する場合があることから、このとき必要となるデータ転送中継の機能を、直結された開放型システム間データを転送する機能（データリンク層）と独立させ、その上位に位置づけておくのが適切であることから設けられている。

【００２２】また、トランスポート層１３、２３はＯＳＩ参照モデルの第４層にあたる層であり、ネットワーク層１２、２２によって構成の複雑なコンピュータネットワークにおいても、終端開放型システムでも、そのネットワークを意識することなく通信を行うことが可能であるものの、通信回線網によっては、転送誤り率やスループットなどサービス品質にばらつきがあるため、そのままでは適用業務が必要とする品質のサービスを提供できないことがあることから、これを補完し、かつ種々の通信網を利用して開放型システム間接続を可能にするためには、ネットワーク層１２、２２の上位に終端開放型システム間でのデータ転送制御を実現する機能層が必要になることから設けられている。

【００２３】また、セション層１４はＯＳＩ参照モデルの第５層にあたる層であり、トランスポート層１３以下の機能によって開放型システム間の効率の良いデータ転送が可能であるものの、応用プロセスが意味のある通信を行うためにはさらに、応用プロセス間で合意された一定のルールに従って秩序正しくデータを送受信する機構、すなわちトランスポート層１３の上位に、業務の目的に合わせて応用プロセス間で種々の形態の対話を可能する機能が必要になることから設けられている。

【００２４】また、プレゼンテーション層１５はＯＳＩ参照モデルの第６層にあたる層であり、セション層１４を利用すれば応用プロセス間でのデータの送受信は可能になるものの、応用プロセスがそのデータを正しく処理するためには、データの表現形式（符号・キャラクタセット、データ圧縮、暗号など）に対する解釈の相違が発生しないようにする必要、すなわちセション層１４の上位の機能層として、データの表現形式の折衝・識別・解釈などを行い、必要に応じて表現形式の変換も行う機構を設定しておく必要があることから、このデータ表現形式制御の機能として、データの意味内容を扱う機能と切り離しておくのが適当であり、これによってデータの意味内容を変更することなく、適切な表現形式を採択してデータを送受信することが可能になることから設けられている。

【００２５】また、応用層１６はＯＳＩ参照モデルの第７層にあたる層であり、応用プロセス間で送受信されるデータの意味内容に対応した通信処理機能を行うのみならず、通常の適用業務では、資源利用機能（例えばファイル転送・アクセス、データベースアクセス、仮想端末アクセス、メールボックスアクセスなど）と、コンピュータネットワークの運転制御に必要なネットワーク管理機能（開放型システムや物理媒体などに対する障害管理、構成管理など）とを必要とすることから、応用プロセスの処理内容に対応した通信処理機能として、データの意味内容にかかわらないプレゼンテーション層１５以下の層に対し、別の機能層として設定しておく必要があることから設けられている。

【００２６】そして、セキュリティレベルが低い第１ＬＡＮ３を構成する端末装置２の１つからセキュリティレベルが高い第２ＬＡＮ６を構成する端末装置５に対して接続要求を出したとき、図４に示す如くＬＡＮ間接続装置７のトランスポート層２３によってこれを取り込んで接続要求のＴＣＰフォーマットおよびこのＴＣＰフォーマット中の確立要求フラグの有無を確認するとともに、この確認結果に関わらず接続要求を出した端末装置２と、接続先として指定された端末装置５との間のコネクションを禁止する。

【００２７】逆に、セキュリティレベルが高い第２ＬＡＮ６を構成する端末装置５の１つからセキュリティレベルが低い第１ＬＡＮ３を構成する端末装置２に対して接続要求を出したとき、ＬＡＮ間接続装置７のトランスポート層２３によってこれを取り込んで接続要求のＴＣＰフォーマットおよびこのＴＣＰフォーマット中の確立要求フラグの有無を確認し、正しい接続要求であれば、接続要求を出した端末装置５と、接続先として指定された端末装置２との間のコネクションを確立してデータ通信を行なわせる。

【００２８】これによって、第２ＬＡＮ６の各端末装置５によって第１ＬＡＮ３を構成する他の各端末装置２内のデータを参照したり、より大規模なデータ処理を可能にしたりする。

【００２９】このようにこの実施例においては、セキュリティレベルが高い第２ＬＡＮ６を構成する各端末装置５からセキュリティレベルが低い第１ＬＡＮ３を構成する各端末装置２に対するデータアクセスがあったとき、ＬＡＮ間接続装置７のトランスポート層２３によってこ

れを検出してこれらの各端末装置２、５間のデータアクセスをサポートし、逆にセキュリティレベルが低い第１ＬＡＮ３を構成する各端末装置２からセキュリティレベルが高い第２ＬＡＮ６を構成する各端末装置５に対するデータアクセスがあったとき、ＬＡＮ間接続装置７のトランスポート層２３によってこれを検出してこれらの各端末装置２、５間のデータアクセスを禁止するようにしたので、セキュリティレベルが異なるＬＡＮ間を接続するとき、セキュリティレベルが低い方のＬＡＮからセキュリティレベルが高い方のＬＡＮに対する不正なデータアクセスを防止し、これによってセキュリティレベルが高く設定されているＬＡＮのデータが外部に漏れないようにすることができる。

【００３０】

【発明の効果】以上説明したように本発明によれば、セキュリティレベルが異なるＬＡＮ間を接続するとき、セキュリティレベルが低い方のＬＡＮからセキュリティレベルが高い方のＬＡＮに対する不正なデータアクセスを防止し、これによってセキュリティレベルが高く設定されているＬＡＮのデータが外部に漏れないようにすることができる。

【図面の簡単な説明】

【図１】本発明によるＬＡＮ間接続装置の一実施例を使用した情報処理ネットワークシステムの一例を示すブロック図である。

【図２】図１に示す第１、第２ＬＡＮおよびＬＡＮ間接続装置の構成例を示す模式図である。

＊【図３】図１に示す第１、第２ＬＡＮおよびＬＡＮ間接続装置の各層を説明するための模式図である。

【図４】図１に示す情報処理ネットワークシステムの動作例を示す模式図である。

【図５】従来から知られているＬＡＮ間接続装置を使用した情報処理ネットワークシステムの一例を示すブロック図である。

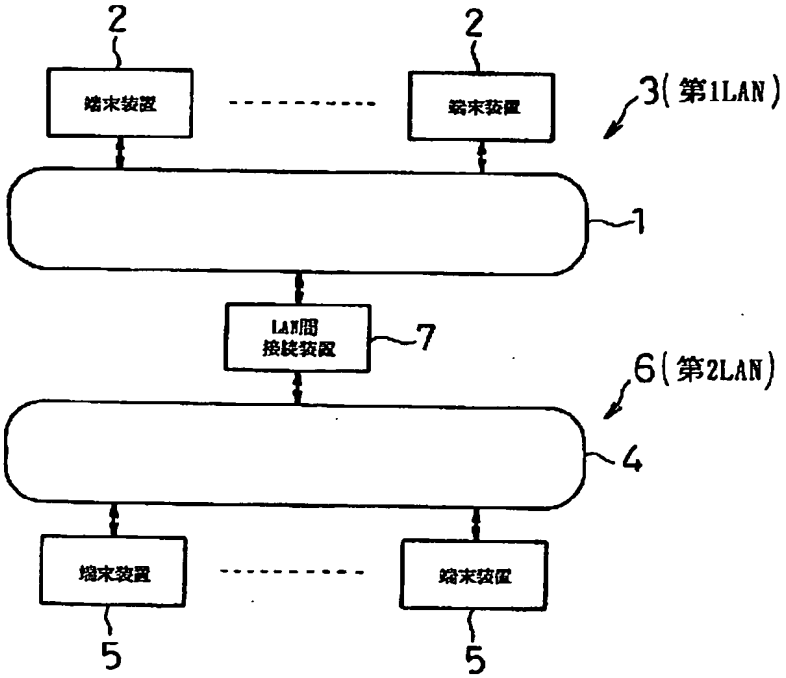
【図６】図５に示す第１、第２ＬＡＮおよびＬＡＮ間接続装置の構成例を示す模式図である。

【図７】図５に示す情報処理ネットワークシステムの動作例を示す模式図である。

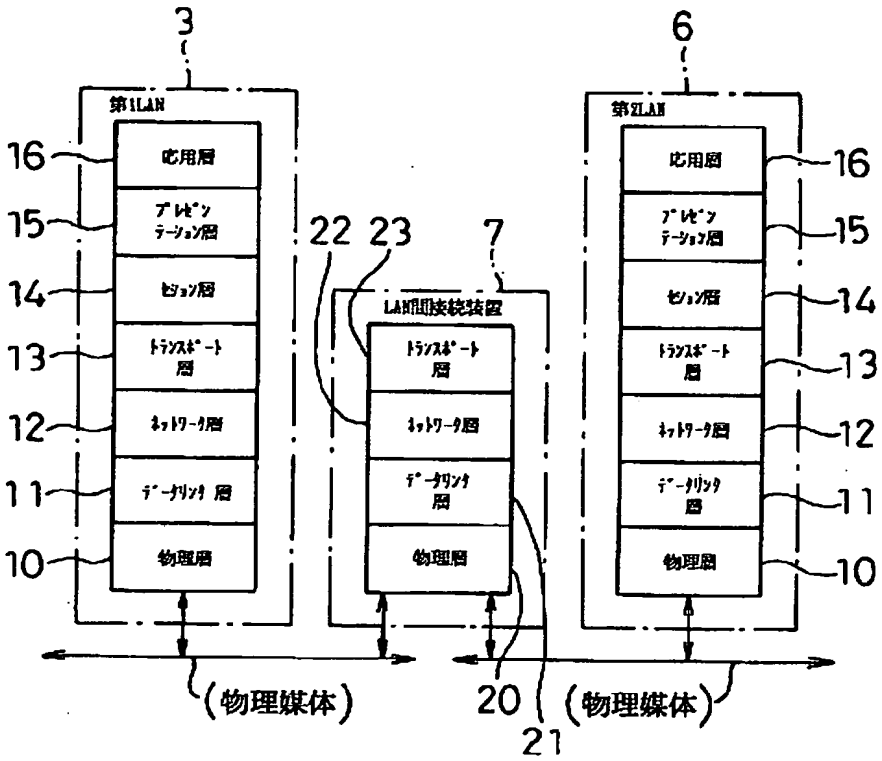
【符号の説明】

１　ケーブル
２　端末装置
３　第１ＬＡＮ（低セキュリティＬＡＮ）
４　ケーブル
５　端末装置
６　第２ＬＡＮ（高セキュリティＬＡＮ）
７　ＬＡＮ間接続装置
１０、２０　物理層
１１、２１　データリンク層
１２、２２　ネットワーク層
１３、２３　トランスポート層
１４　セション層
１５　プレゼンテーション層
１６　応用層

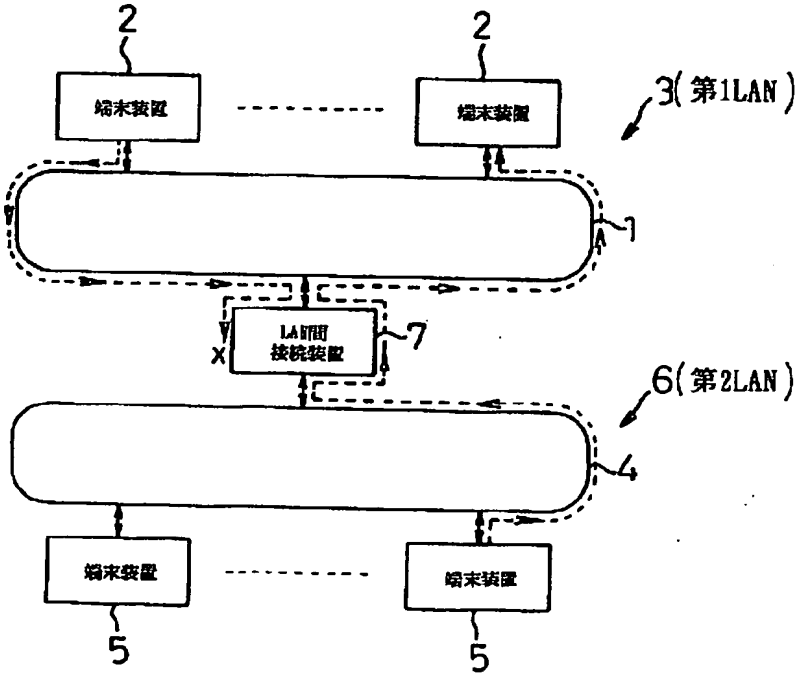
【図１】



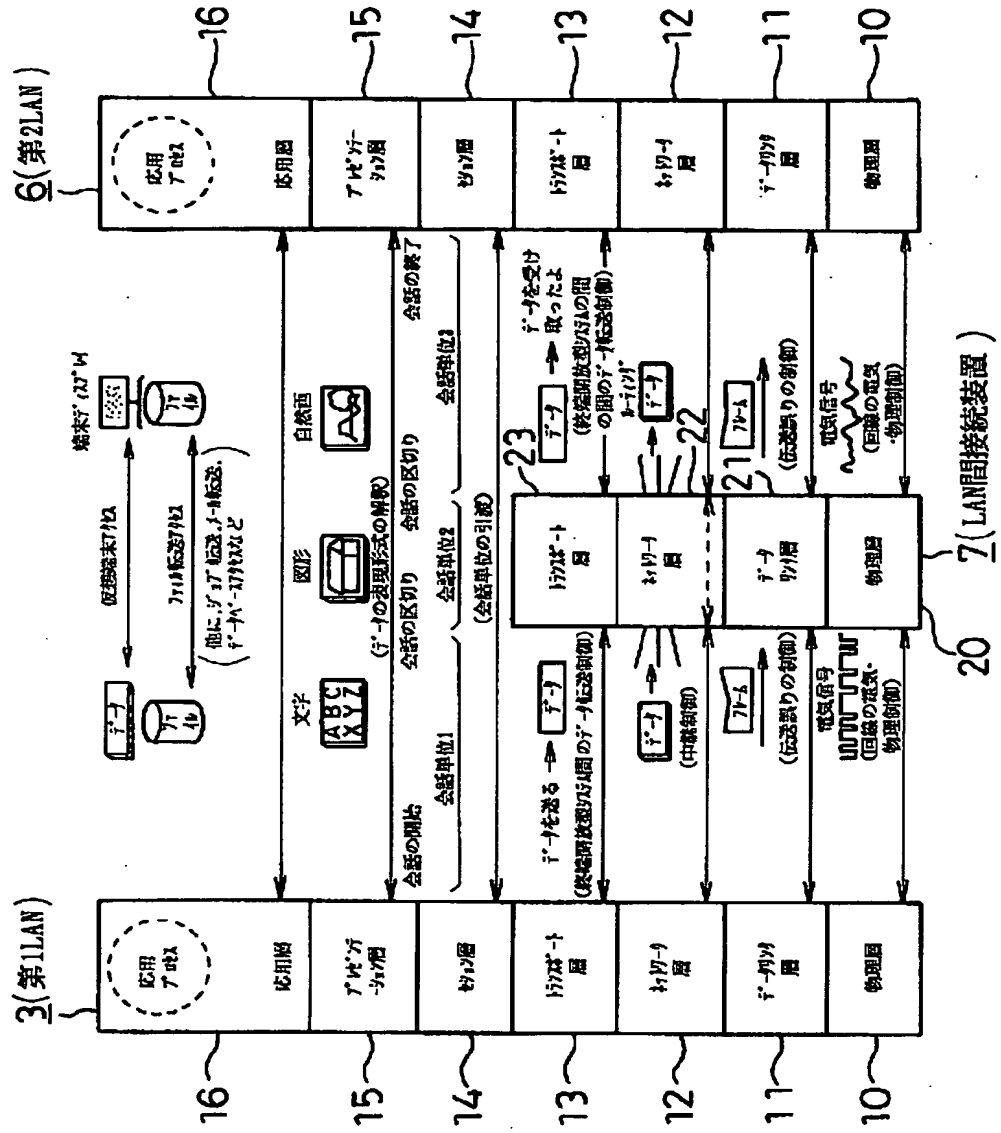
【図２】


3
6
第1LAN
第2LAN
応用層
プレゼンテーション層
セション層
トランスポート層
ネットワーク層
データリンク層
物理層
16
15
14
13
12
11
10
22
23
7
LAN間接続装置
(物理媒体)
20
21
(物理媒体)

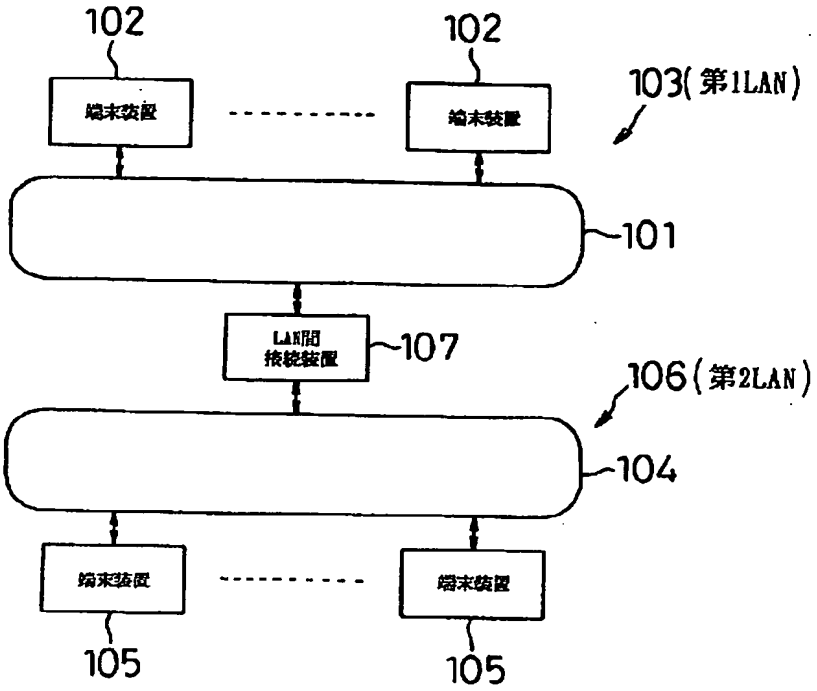
【図４】


2
2
端末装置
端末装置
3(第1LAN)
1
LAN間接続装置
7
X
6(第2LAN)
4
端末装置
端末装置
5
5

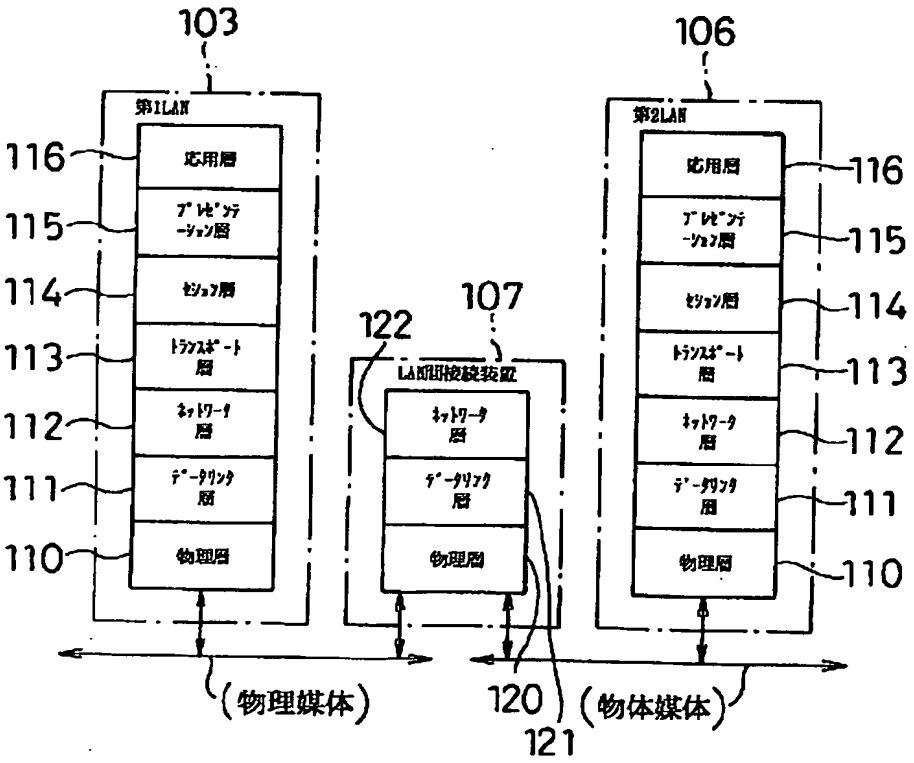
【図３】


6(第2LAN)
3(第1LAN)
7(LAN間接続装置)
20
16
15
14
13
12
11
10
応用層
プレゼンテーション層
セション層
トランスポート層
ネットワーク層
データリンク層
物理層
応用プロセス
仮想端末プロセス
ファイル転送プロセス
他に、ジョブ転送、メール転送、データベースアクセスなど
端末データ
ファイル
データ
文字
図形
自然画
ABC XYZ
データの表現形式の解釈
会話の開始
会話の区切り
会話の終了
会話単位1
会話単位2
会話単位3
(会話単位の引数)
データを送る
(仮想端末プロトコルの)データ転送制御
データを受け取ったよ
(仮想端末プロトコルの)データ転送制御
データ
(中継制御)
フレーム
(伝送誤りの制御)
電気信号
(回線の電気・物理制御)
22
21
23

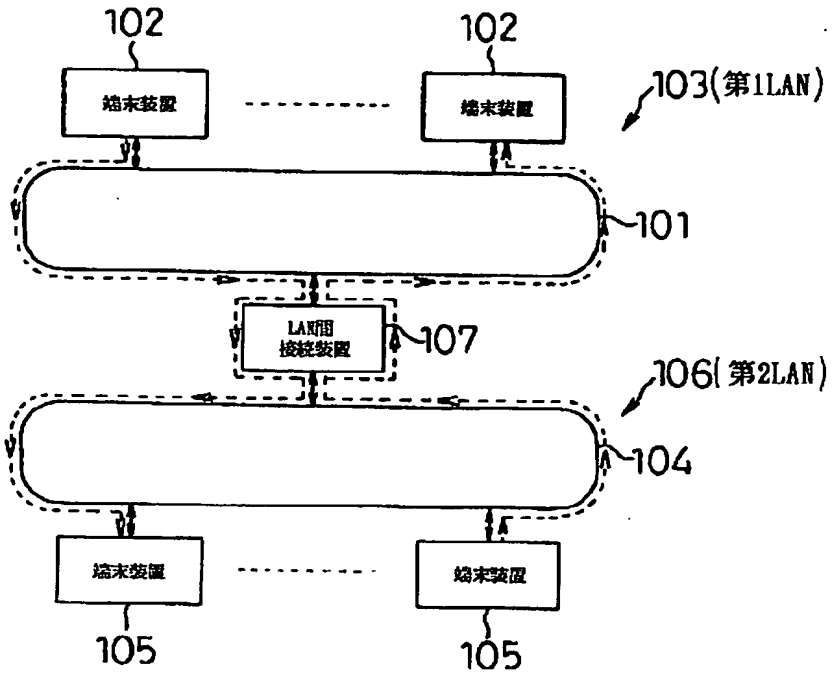
【図５】


102
102
端末装置
端末装置
103(第1LAN)
101
LAN間
接続装置
107
106(第2LAN)
104
端末装置
端末装置
105
105

【図６】


103
106
第1LAN
第2LAN
応用層
プレゼンテーション層
セション層
トランスポート層
ネットワーク層
データリンク層
物理層
116
115
114
113
112
111
110
107
122
LAN間接続装置
(物理媒体)
120
121
(物体媒体)

【図７】


102
102
端末装置
端末装置
103(第1LAN)
101
LAN間
接続装置
107
106(第2LAN)
104
端末装置
端末装置
105
105